FJ-H337-DE

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/30, G06F 13/362

A1

(11) International Publication Number: WO 99/35783

(43) International Publication Date: 15 July 1999 (15.07.99)

(21) International Application Number: PCT/US99/00344

(22) International Filing Date: 6 January 1999 (06.01.99)

(30) Priority Data:

60/071,084	9 January 1998 (09.01.98)	US
09/085,437	27 May 1998 (27.05.98)	US

(71) Applicant: CYBERSAFE CORPORATION [US/US]; Suite 310, 1605 N.W. Sammamish Road, Issaquah, WA 98027–5378 (US).

(72) Inventors: HUR, Matthew; 1010 13th Place S.W., North Bend, WA 98045 (US). MEDVINSKY, Gennady; 14266 S.E. 6th Street, Bellevue, WA 98007 (US). KOVARA, Joseph, N.; P.O. Box 1027, Issaquah, WA 98027 (US).

(74) Agents: HANSRA, Tejpal, S. et al.; Sheridan Ross P.C., Suite 3500, 1700 Lincoln Street, Denver, CO 80203–4501 (US).

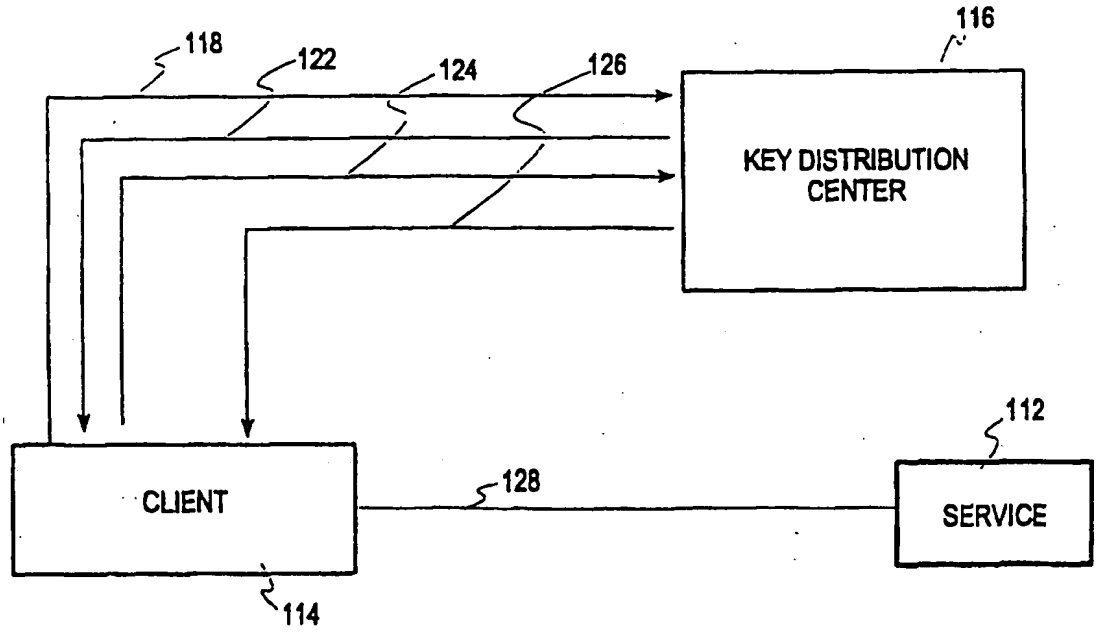
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CLIENT SIDE PUBLIC KEY AUTHENTICATION METHOD AND APPARATUS WITH SHORT–LIVED CERTIFICATES



(57) Abstract

An authentication system with an ability to effectively implement a system for providing short–lived certificates is described. A key distribution center (KDC) (116) generates and stores public private key pairs and certificate templates. A user is assigned a user public private key pair which is stored in the KDC (116). A user (114) who authenticates to the KDC (e.g. using a password according to, e.g., a kerberos system) prompts the system to recertify the user's public key by generating and signing a short–lived certificate.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

CLIENT SIDE PUBLIC KEY AUTHENTICATION METHOD AND APPARATUS WITH SHORT-LIVED CERTIFICATES

The present invention is directed to a public key authentication system and, in particular, to a system making it practical to implement client side public key authentication.

BACKGROUND INFORMATION

One of the earliest information security systems was the development of ciphers and systems of encryption and decryption for the purpose of assuring privacy (protecting information from unauthorized readers). More recently, and especially with the introduction of electronic communication and computer-based information systems, information security systems have also been used for other purposes such as authentication (assuring that a message truly originated at its purported origin) and authorization (preventing access to hardware, software or data by unauthorized persons). The present invention, although having applicability or relationships in many areas of information security, is most apparently directed toward client side public key authentication. Typically, after authentication has occurred, the authentication can form a basis for later decisions, such as making access control decisions.

Many security systems are fundamentally related to systems of data encryption. The relationship of encryption to information privacy is apparent, although systems for encrypting and decrypting data have developed to include many elaborate schemes. Encryption can be related to identification and authentication in a number of ways. Most apparently, if the receiver of an encrypted message trusts that only one other person possesses the key by which the message was encrypted, then identification and, to some extent, authentication, is achieved upon successful decryption. By using encryption for authentication purposes, its role in access control is apparent since control to a resource can be predicated upon authentication of the person seeking access. In a password-based authentication system, encryption may play a role in avoiding disclosure of passwords to unauthorized parties (such as by encrypting passwords before they are transmitted or stored, or transforming the password into a symmetric key and using it in an encryption based protocol to authenticate the user).

Encryption systems are often categorized into secret key ("symmetric key") systems and public key ("asymmetric key") systems (sometime called a public-key private-key system), although there are other systems, as well. In a typical secret or symmetric key system, the same key is used for both encrypting and decrypting. In this system, it is important to maintain secrecy of the key, (albeit a shared secret) e.g., such that only authorized persons have knowledge or possession of the shared secret key. Thus, one of the difficulties with the secret key system is maintaining key secrecy. Another problem is key proliferation. If a party wishes to have private communication with two or more other parties but does not necessarily wish all parties to have access to all such communications, it will, in general, be necessary to have a different secret key shared between each pair of persons. Maintaining and distributing such keys becomes unwieldy in large organizations. One approach is to establish a trusted third party (TTP) in such a fashion that would require each party to have only a single key: that between himself and the TTP, with the TTP acting as an intermediary to establish any particular desired communication channel. This system, while useful for many purposes, presents difficult problems of how to assure security of the TTP itself and maintaining the host's key secret. One implementation of a TTP which has achieved some degree of success is that generally known as kerberos, described more thoroughly below. In general, a "kerberos-like system," as used herein, refers to kerberos and any trusted third party system that shares symmetric keys with users and services. Although a kerberos-like system has been found highly useful in a number of situations, it is believed that previous kerberos-type systems typically have not been deployed so as to provide advantages associated with public key systems (such as, e.g., digital signatures).

In a public key (PK) system, two corresponding ("asymmetric")keys are used in connection with protecting information. Information which is encrypted with one of the two keys can be decrypted only with the other key. In some public key systems, either of the two keys can be used to encrypt and the other key to decrypt. In other systems, one key must be used only for encryption and the other only for decryption. One important feature of public key systems is that it is computationally infeasible to use knowledge of one of the keys to deduce the other key. In a typical public key

system, each user of the system possesses a set of two such keys. One of the keys is maintained private while the other is freely published. If a sender encrypts a message with the recipient's public key, only the intended recipient can decrypt the message (since only the recipient is in possession of the private key corresponding to the published public key). If the sender, before performing the above encryption, first encrypts the message with the sender's private key, the recipient, upon performing first a decryption (using the recipient's private key), then a decryption on the result (using the sender's public key) is assured not only of privacy but of authentication since only the sender could have encrypted a message such that the sender's public key successfully decrypts it. In one digital signature scheme, a one-way hash is first applied to a message and the hash of the message is encrypted with the sender's private key.

In this scenario, the degree of confidence that the recipient has in the source of the message depends on the degree of the recipient's confidence that the sender's public key corresponds to a private key that was possessed only by the sender. In many current systems, a number of generally well-trusted certification authorities have been established to provide this degree of confidence. In the system currently in widest use, these authorities provide public key certificates. Under the most widely used certificate standard (Standard X.509 developed by the International Standards Organization (ISO) and the Comité Consultatif Internationale Telegraphique et Telephonique (CCITT)), such certificates include a public key, the name of the person who possesses or is associated with the public key, and other information which may, e.g., include an expiration date, all of which are digitally signed by a trusted party (and are thus in encrypted or otherwise modified form). The digital signature may be provided, e.g., according to the digital signature standard (DSS) (National Institute of Standards and Technology (NISD)). Typically, a digital signature involves applying a one-way hash and then encrypting with the private key of, in this case, the certification authority. Such digital signature is provided using the private key of the trusted party which, in turn, is authenticated using the trusted party's certificate signed by yet another trusted party, so that there may be a multi-level hierarchy of trusted parties.

Although public key systems are used in a number of situations, including certain Internet browsing situations, experience has shown that public key systems can have their own difficulties. To provide an acceptable level of security, the key which a user maintains secret is not feasible to remember (typically being a large number such as a 1024-bit binary number) and thus, to be practical, must be stored, making it vulnerable to breach of security and, in many systems, requiring use of a particular piece of hardware (e.g., a Smartcard or, in some cases, a particular computer).

In one previous system, a Smartcard formed part of an authentication system. A number of Smartcard systems and uses are known. For example, the Secure Socket Layer (SSL) protocol requires a digital signature for a client application to establish communication with certain services. In some environments, a Smartcard will hold information used to provide such a digital signature, so that users can access such resources if they possess an appropriate Smartcard (and without the need to, e.g. memorize a key). Other Smartcard authentication procedures using public and private key pairs are also known. The principle Smartcard interfaces currently in use are PKCS #11 (Public Key Cryptography Standard, RSA Data Security, Inc.) and PC/SC (Personal Computer/Smartcard).

As noted above, a certificate is typically provided with an expiration date. Such expiration dates typically are on the order of a year or more from issuance, thus making certificates, in current systems, relatively long-lived. There are number of reasons for this. One of the features that makes a public key system attractive is its ease of use, and it would be counter to this goal if users had to obtain key pairs and publish new public keys on a very frequent basis. Nevertheless, in some circumstances, it is desirable to revoke a previously published certificate. For example, a public key pair which is used to control an employee's access to sensitive company information might be revoked when the employee leaves the company. Accordingly, previous public key systems have typically come to rely on checking certificates against a certificate revocation list (CRL). The X.509 standard provides an example of CRL representation. Unfortunately, this requires distribution, e.g. intranet- or Internet-wide distribution, of CRLs, and requires an additional checking

or comparison step. These items can be burdensome or even render the system infeasible in relatively large enterprises or networks.

Another difficulty associated with public key systems is distribution and management of the private keys. For example, as a company hires new employees, it may want to provide some employees with public-private key pairs, but it becomes problematic to distribute the private keys in such a manner as to avoid revealing the private keys to other parties. Although employees' private keys should remain private if they are to serve the intended purpose, there are circumstances where a company may need to access such keys (e.g. to obtain company-owned information which was encrypted by a now-deceased employee). However, maintaining a employees' keys, e.g., in escrow would typically involve substantial management effort and expense.

Accordingly, it would be useful to provide a system in which public key technology can be used, e.g., for securing computer networks while reducing or eliminating the burden of the CRL-checking system, without compromising security (e.g., form departed employees or others who, under a conventional system, would have their certificates revoked). It would also be useful to provide a system which reduces or eliminates the effort and expense associated with private key distribution and management. It would further be useful to provide a public key system in which the goal of private key storage can be achieved while reducing or eliminating the hardware-dependence and/or security risks associated with previous systems.

Additionally, it would be useful to provide such an improved public key system while taking advantage of features of already-used systems to minimize the amount of development, programming and changes to current systems in order to implement such features.

SUMMARY OF THE INVENTION

The present invention provides a system for automatically generating short-lived public key certificates (PKC), i.e. with a validity period less than 1 month preferably less than 1 week, more preferably less than 1 day and even more preferably less than about 12 hours, e.g., for session-oriented authentication or other security purposes, such as authorization. In one embodiment, each time a user authenticates using a first

authentication system (e.g., every time a user logs onto the system and authenticates him or herself), a new but short-lived PKC will be generated and delivered to the user. It is anticipated that typically, the public key will be re-certified relatively frequently (e.g. every 8 hours, every workday, etc.); the public-private key pair itself remains unchanged, and is relatively long-lived (e.g. with a lifetime of about 1 year or more). This newly generated PKC can then be used in a fashion similar to that for which PKCs were used in previous systems, including systems for controlling access to resources such as web pages or other resources.

In one embodiment, the system not only delivers the short-lived PKC but also delivers the private key corresponding to the PKC's public key. This relieves the user from having to be responsible for storing a public key or from being restricted to using particular hardware on which the private key is stored (although such a hardware-based approach could be used if preferred). Because the PKC is short-lived, it is possible to achieve a relatively high degree of trust without the need (or with a reduced need) for processing CRLs. In the case of, for example, a departed employee, the system will be configured to refuse to issue any more (short-lived) certificates for such employees and because previously-valid issued certificates will have expired (or will shortly expire), checking against a CRL is unnecessary.

In one embodiment, since both the private key and public key are returned to the computer of the person seeking access, it is possible, if desired, to implement a simulated Smartcard in which the private key and public key, cached locally in the computer of the person seeking access, are used to simulate the presence of a physical Smartcard. For example, in connection with a PKCS #11 interface, the simulation can take the form of fulfilling Smart API Calls such as, e.g., C-SIGN, C-VERIFY. In this way, the present invention can take advantage of relatively mature application programming interfaces (APIs) for Smartcards to implement a public key-based, client side authentication, without the need for actual Smartcard hardware (such as without the need for users to obtain and carry actual Smartcards).

In one embodiment, a TTP system which may be, for example, similar to a kerberos system, can be adapted for use as the short-lived certificate generating system. Such a system combines some of the advantages of a kerberos-type system, such as

being password based and tolerant of users who log on at different computers ("roving users") with certain advantages of a public key system (such as facilitating access to resources which are protected via a public key infrastructure or system) while avoiding the above-noted difficulties with public key systems, such as private key distribution and management difficulties, the need for maintaining and using CRLs and storing private keys in relatively insecure or inconvenient fashions.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic block diagram of a kerberos-type system according to previous procedures;

Fig. 2 is a flowchart of a public key/Smartcard authentication system according to previous systems;

Fig. 3 is a flow chart depicting certificate generation and use according to an embodiment of the present invention;

Fig. 4 is a block diagram of certain components of a system illustrating use of the procedure of Fig. 3;

Fig. 5 is a block diagram of a system for use with a simulated smartcard and/or a hardware smartcard, according to an embodiment of the present invention;

Fig. 6 is a block diagram of a system for use with a simulated smartcard and/or a hardware smartcard, according to an embodiment of the present invention;

Fig. 7 is a block diagram illustrating a system for logging in to a simulated smartcard, according to an embodiment of the present invention;

Fig. 8A and 8B are block diagrams illustrating examples of how a system according to the present invention can provide support for third-party Public Key Infrastructures (PKI); and

Fig. 9 is a block diagram illustrating user enrollment in the context of a simulated smartcard system, according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Before describing features of embodiments of the present invention, certain features of previous systems will first be described. Fig. 1 depicts an authentication

procedure using a kerberos system. Although the kerberos system uses a password for authentication, the system is particularly secure because it never transmits passwords, either encrypted or unencrypted, over the network. In the depicted embodiment the system can provide a number of different services, including a ticket-granting service (described below) and various other services that may be desired by the user. In the depicted embodiment, the person who desires to use a particular resource or service 112 (which may be, for example, a software service such as a particular application program, may be data, may be a particular hardware resource or combination thereof) attempts to log onto the system, entering (usually in response to a prompt) a password known only to the person being authenticated. Preferably, for a typical user session, this is the only time the user will need this password during a (normal-length, e.g. 8-10 hour) session (although, if desired the system can be configured to require re-input of the password to perform certain tasks, such as administration tasks on the security system). The person makes the log-on attempt using a client computer 114 coupled, e.g., via a local area network (LAN) or other communication system to a key distribution center (KDC) 116. In response, the client 114 sends a request message (AS-REQ) 118 to the KDC. The request 118 indicates the name of the person requesting the service but does not include the password. The KDC 116 responds 122 with an encrypted "ticket granting ticket" (TGT) (AS-REP). The ticket granting ticket includes two main components: a ticket for the client to use the ticket granting service (the majority of which, including the session key, is encrypted with the key of the ticket granting service) and a session key for the client and ticket granting service, encrypted with the client key. When the user wishes to begin using a particular service 112, an additional transaction with the KDC is needed. The client computer 114 transmits a ticket request 124 (TGS-REQ) to the KDC 116. The request includes a number of components including an authenticator (generated by the client) for the client to use the service, encrypted with the session key(the session key is sealed in the TGT); the ticket for a client to use the ticket granting service, the majority of which is encrypted with the key of the ticket granting service (both of which were included in the ticket granting ticket 122) and the name of the service 112. In response, the key distribution center 116 transmits to the client a ticket 126 (TGS-REP) (the majority of

which is encrypted) which contains a ticket for the client to use the server, at least partially encrypted with the server's key, and a copy of the session key, encrypted with the session key that is shared between the client and the ticket granting server. At this point, the client now has sufficient items to gain access to the service 112 as desired. This is achieved by transmitting from the client to the service 112 a message containing an authenticator and a ticket. In response, the service provides the desired server response to the client. The service 112 can treat the ticket as authentic because only the KDC and the service 112 share the secret key with which the ticket is encrypted.

As depicted in Fig. 2, a public key system operates in a substantially different form. Typically a user generates a public-private key pair 202. The user stores the private key 204 in any of a number of fashions, such as in a file on a client computer or on a Smartcard. Such storage in previous systems is believed to raise difficulties. Storing in a file located on a particular computer impairs "roving users" since the user can only use or access his stored private key on the particular computer where it was stored. That is, the system is inconvenient or infeasible for users who need or desire the ability to log onto any of a plurality of different computers (e.g., any of a plurality of nodes in a local area network or other network) and still be able to use a public key system-controlled resource. It is further believed that storing private keys in a file on a computer, even if protected by encryption or other measures, represents a security vulnerability of the system. Storage of a private key on a Smartcard is at least theoretically compatible with roving users but in many situations is infeasible because of the cost and administrative overhead involved in equipping a plurality of machines with Smartcard readers and distributing Smartcards to various users.

The user submits the public key for certification to a trusted entity such as a certification authority (CA), e.g. via a PKCS #10 request. Upon verifying the requestor's identity (out of band) the CA issues an X.509 certificate to certify the user's public key 212. The certificate is then sent back to the user and typically will be publicly available, such as by publication in a directory such as an X.500 or LDAP (Lightweight Directory Access Protocol) directory, both well-know to those of skill in the art. The CA also periodically issues certificate revocation lists (CRL's) 214 as described above. One mechanism for distributing CRL's is via LDAP.

In certain previous systems, a user wishing to access a resource would retrieve the private key (typically in an automatic fashion) 218. Using any of a number of systems known in the art for public key system based authentication, a resource control device will verify, using e.g. the user's public key (certified by the CA) that the user has been properly and correctly identified 222. Because of the long lifetime of certificates in previous systems, the resource control device will then perform a comparison with the CRL in order to determine whether the certificate has been revoked 224. As noted above, the comparison 224 represents an additional step in the process of controlling access. Additionally, there is an administrative cost in producing, distributing, storing and otherwise tracking CRLs, particularly when CRLs are promulgated with sufficient frequency to detect use of even recently-revoked certificates.

In order to address these and other problems, in previous systems, one embodiment uses a certificate generation system as depicted in Fig. 3. Although, as will be apparent to those of skill in the art after understanding the present disclosure, a number of different systems could be used for generating certificates, in one embodiment a modified kerberos-like system is used. In the embodiment depicted in Fig. 3, one of the components of the modified kerberos-like system is a key distribution center (KDC) 416 (Fig. 4). The key distribution center 416 can be similar to that described in connection with Fig. 1 but modified (e.g. provided with different software) for the procedure described below. In the system and procedure of Fig. 3, initially (e.g. at installation time), the KDC 416 will generate a public-private key pair 312. The system will also generate a certificate template (such as an X.509 certificate) 314. The KDC 416 will then use the KDC's private key to sign the template. These steps 312, 314, 316 are substantially similar to procedures followed by root certification authorities (but not, typically, by network servers or KDC's) in previous systems. When a user registers, the client administration will generate a long-lived public-private key pair associated with that particular user and will store 318 the key pair in the KDC 416, associated with an identifier of the user. When the user begins a session, such as by logging on to a network, the user will enter a password, causing the client 114 to send 322 an AS-REQ message 118 to the KDC 416, as described previously in connection with Fig. 1. In the embodiment of Figs. 3 and 4, in response to the AS-REQ 118, the system will re-certify

the user's public key. Specifically, the system will generate and sign an X.509 certificate for the user 324. Thus, whereas in previous public key systems, a CA would generate and publish a certificate once (upon initial issuance) according to the system of Figs. 3 and 4, the system will generate a certificate containing the user's public key multiple times, typically, each time the user logs on to the system resulting, over time, in a sequence of certificates for this user.

An additional difference between the present system and typical public key systems is that the certificate is short-lived, i.e., contains an expiration time/date which is significantly less than the one- to two-year (or longer) certificate expiration date in previous public key systems, preferably expiring in less than six months, or preferably less than a month, more preferably less than a week, even more preferably less than 24 hours, and yet more preferably expiring less than 12 and preferably around 8-10 hours after issuance. It is anticipated that the expiration date of such short-lived certificates will vary with the needs of the company or other enterprise implementing such systems, and preferably one or more normal or default lifetimes for certificates can be established, e.g. by a system administrator (following proper authentication). It is anticipated that certificate lifetime policies will be set so as to provide certificates with lifetimes sufficiently short that checking against CRL's can be reduced or eliminated without significantly diminishing overall security. Accordingly, each time the system generates (or re-signs) a certificate for this user (i.e. a certificate containing the user's public key) the certificate will have a different expiration time. Typically, a new certificate (based on identical public key) will generate only after the expiration of the previous certificate, although other protocols could also be used. Thus, the result of the present system will typically be issuance of a series or sequence of certificates for any given user (typically on a daily or workday basis) but in which the certificates for this user are not completely identical, i.e. will differ from one another with regard to the expiration time-date (but, for a given user, will have identical public keys). This is in contrast with previous public key systems in which a certificate, once it was issued, was not thereafter issued again for the same public key in a different form or with different information (specifically with different expiration time/date).

In one embodiment, other data may be added to or modified in the series of short-lived certificates for a user. For example, data indicating which resources a given user is authorized to use (or other authorization data) can be included in the short-lived certificates. One example of such authorization information is information indicating one or more user groups with which a user is affiliated, e.g. whose members are authorized to use certain resources. It is believed inclusion of such authorization data, which typically may change on a relatively short time frame, (e.g. days or weeks) would not have been appropriate for inclusion in (and, it is believed, was not included in) previous (long-lived) certificates, but is feasible for inclusion in short-lived certificates according to embodiments of the present invention.

After generation of the certificate, the system will then transmit or deliver 326 the certificate 422 to the client 144. In one possible embodiment, the delivery is made as part of the (modified) AS-REP response, analogous to that described above in connection with Fig. 1.

After the user has logged on and has received the certificate 422, anytime during the valid lifetime of the certificate that the user wishes to authenticate to a resource, including a public key-controlled resource 418, the user can do so, e.g. using the certificate, typically without the need to enter the password again. After the short-lived certificate has expired, in order for the user to authenticate to a resource, the user will need to repeat the procedure described above in order to obtain another short-lived certificate, thus typically requiring re-entering the password.

Preferably, the system delivers not only the certificate, but also the private key of the user 328 (i.e. which corresponds to the public key on which the certificate is based), preferably protected by a shared secret such as a session key generated by the kerberos-like system. In this way, the user is able to retrieve the private key for use as described in Fig. 2 (218) but without having to store the private key in a file on the client computer 114 (where, as noted above, it may be relatively vulnerable). Additionally, by providing a central location for storing users' private keys, central administration of private keys (and implementation of key policies) is made feasible, in contrast to previous PK systems, which were typically based on a paradigm of private keys being widely distributed (i.e. individually stored by individual users). Moreover, since, according to the present

system, a user can use any of a plurality of computers to log onto the system using his or her password, this system supports roving users, but without the requirement for a physical Smartcard. The client computer 114, being in possession of both the private key and the certificate, can access 332 a public key controlled resource 424.

A public/private key pair may be used in connection with authenticating to a number of resources. As one example, an access control decision can be made based on an authentication process which involves use of a Smartcard, e.g. using a hardware Smartcard 516 in connection with a Smartcard interface 518 such as a PKCS #11 application programming interface 512 (Figs. 5 and 6). However, the present invention affords an additional opportunity. According to the embodiment generally illustrated in Fig. 5, it is possible to provide a simulated Smartcard/Smartcard interface in place of, or, as illustrated, in addition to, the hardware Smartcard 516 and interface 518. From the perspective of the application 514 (such as, for example, a browser 517) and API 512, there will be no difference between a simulated Smartcard/Smartcard interface 522 and the hardware Smartcard/interface 516, 518. When a user is logging into the card (e.g. using the C-LOGIN call in the PKCS #11 API), the user's password will be used to authenticate to the KDC 416 and retrieve the private key and a freshly generated X.509 certificate 422. These credentials are then cached locally 524 (or remotely). From the cache 524 the credentials may be used to fulfill Smartcard API calls (e.g. C-SIGN, C-VERIFY). The approach of Figs. 5 and 6 permits transparent access to an application 514 via a PKCS #11 API, i.e. using a relatively mature API but without the cost and administrative overhead associated with hardware Smartcards.

As illustrated in Fig. 7, in one example, a process for logging in to a simulated smartcard may begin when a client application 514 uses a standard API such as PKCS #11, MS-CAPI, CDSA and the like, to initiate log on of user into a smartcard. Preferably the process of the present invention is transparent to the client application 514 in the sense that the messages and/or data sent from and received by the client application during the process will be the same regardless of whether the client application 514 is logging on to the simulated smartcard as depicted in Fig. 7 or logs on to a physical smartcard. The particular interface 512 which is used will typically depend on what client application 514 is performing the login (e.g. it is likely a Microsoft® would use an MS-CAPI interface

while other browsers or applications might use PKCS #11 or other interfaces 712). In the illustrated embodiment, the simulated smartcard client 714 (implemented with software typically residing on a client side computer) will authenticate to 716 a security server 718, typically an authentication service such as a Kerberos-like authentication service. Typically, the simulated smartcard client 714 will request a password and/or login name from the user before formulating and sending an authentication request 716. The security server 718 responds by sending 722 authentication credentials to the simulated smartcard client 714. The authentication credentials which are sent 722 may include those described above in connection with the embodiments of the present invention and/or previous systems. However, preferably the information sent 722 is sufficient to permit the simulated smartcard client 714 to send a message 724 to a simulated smartcard server 726 sufficient to authenticate to the simulated smartcard server. Typically the information 722 sent to the simulated smartcard client 714 will include a ticket (generally as described above) for the smartcard service. In response to receipt of an authenticated request 724, the simulated smartcard server 726 returns a (preferably encrypted) smartcard image 728.

As used herein, the "smartcard image" includes at least some information which, in a physical smartcard system, would be stored on or derived from a physical smartcard. Examples include public keys, private keys, symmetric keys, certificates and the like. In one embodiment, the smartcard image is encrypted, for example with a private key. The simulated smartcard client 714 will then decrypt the smartcard image. The decrypted image may contain, e.g., public keys, private keys, symmetric keys, certificates and similar information. Some or all of the information (preferably including especially sensitive information such as a private key) may be encrypted under a password known only to the end user.

In general, in Fig. 7 through 8, blocks shown underneath the client application 514 are items which are client side items, i.e. which use or constitute software residing, typically, on a PC or other computer used by an end user, while items on the right side of the figure represent server-side items i.e. which use or constitute software residing at remote locations such as remotely located network servers. Although, in the embodiment depicted in Fig. 7, a security server 718 and simulated smartcard server 726 are shown as separate blocks, it is also possible to configure a system in which one or more of the

components depicted as separate blocks are, in fact on a single server computer, e.g. in which the security server 718 and simulated smartcard server 726 are located on a single server computer. It is possible, in this situation, to combine steps 2, 3 and 4 so that the simulated smartcard client 714 sends an authentication request 716 to the security server/simulated smartcard server which responds by sending a (preferably encrypted) smartcard image 728 back to the simulated smartcard client 714.

After receiving the smartcard image, the smartcard client 714 will then check for expired public key certificates on the (decrypted) smartcard image. If an expired certificate is found, the simulated smartcard client 714 will submit a re-certification request 732 to a server-side certification authority 734. Typically certifications returned to the simulated smartcard client 714 will be short-lived certificates generally as described above. The simulated smartcard client 714 will then use the objects on the smartcard image to fulfil cryptographic operations provided by the cryptographic API's 512 responding 736 to the client application 514 in a manner substantially identical to the manner of response that would have been provided had a physical smartcard system been used.

After a simulated smartcard login as depicted in Fig. 7, further smartcard operations may be involved in executing the client application 514. Figs. 8A and 8B provide two (of many) possible examples of such further operation. In the example of Fig. 5A, following login and download of the smartcard image 812 (performed generally as described above in connection with Fig. 7), the client application 514 may, e.g., generate or store public key credentials 814 (typically using standard cryptographic API's 512). Such public key credentials are, in the embodiment of Fig. 8A, handled in a fashion which is transparent to the client application 514. In the depicted embodiment, the simulated smartcard client 714 will send a message 816 to the simulated smartcard server 726 to update the simulated smartcard image on the server side. This illustrates one fashion of incorporating a third party's credentials in the system of the present invention and accordingly providing support for third party certification authorities.

Fig. 8B provides another example. In the embodiment of Fig. 5A the client application 514 communicates with a third party certification authority 822, 824 which is neither on a client machine nor a server of the present security system. For example, the

client application 514 may contact a third party certification authority to get certified. However, after such communication 822, when the client 514 sends a message 814' for smartcard storage, the present system provides for simulated smartcard storage, in a manner similar to that described above in connection with Fig. 8A, by sending the information 816' prime to the simulated smartcard server 726 for storage.

Fig. 9 illustrates use of the system, according to an embodiment of the present invention, for enrolling new users in the simulated smartcard system. In the embodiment of Fig. 9, an administrator, e.g. using an administrator server 912, prepares a certificate template (preferably assisted by software for generating such templates) which is sent for storage 914 on a simulated smartcard server 726 (or a storage device 916 associated therewith). The template specifies at least some of the components of the certificate for use in the system. Typically, the template will contain, e.g., the user's distinguished name, the issuer's distinguished name and the like. An initial password is generated for a new user and stored on the security server 718 (or a storage device couple therewith) preferably resetting the password 722 such that after the user preforms an initial log on, the password will be flagged as being in an expired state (thus forcing the user to change the password).

The generation of a new public-private key pair for the user could be performed either on the client side computer 714 or on a server (e.g. 912). Client side key generation might be used when it is desired to reduce the computing load on server computers. However, particularly in situations where many users are being added at one time, it may be useful to generate the new pairs on the server side 912 to facilitate setting up the system to accommodate a number of new users. The passwords discussed above are distributed to the various users. Preferably this is done out-of-band (without transmitting the password over the computer network, such as by providing the password in a personal meeting, over the telephone and the like). As each new user logs into the system for the first time 922, the user preferably will be required to change his or her password (as described above). If the key pair was not previously generated on the server side, the simulated smartcard client 714 will generate the key pair. The smartcard image is then downloaded to the client, e.g. using a procedure 812 similar to that described above. The keys are then generated and written back to the smartcard image on the server

side, e.g. using a procedure 816 similar to that described above in connection with Fig. 8A.

In light of the above description, a number of advantages of the present invention can be seen. The present invention provides a turnkey solution making public key authentication feasible. In one embodiment, the present invention employs a symmetric key authentication to enable use of an application which may be protected by an asymmetric key system. The present invention makes it practical to implement client side public key authentication by solving the private key management and certificate revocation problems. The invention provides for public key authentication without the need for (or with reduced need for) CRLs and/or without the need for client-stored or smartcard-stored private keys. The present invention provides for relatively frequent public key recertification (e.g. every work day) without the need for frequent regeneration of new key pairs, which is a computationally expensive operation. The present invention can be implemented using (in modified fashion) certain previous systems or standards such as a modified kerberos and/or PKCS #11, MS-CAPI or CDSA implementations, thereby taking advantage of certain relatively mature or developed systems (or features of such systems) while avoiding certain disadvantages previously considered to be an unavoidable part of such systems. The present invention provides an opportunity to implement central administration of both a public key system and kerberos system to accommodate both types of uses. The present invention provides a single system which can both use or implement a public key system and act as a certification authority.

A number of variations and modifications of the present invention can also be used. Although the depicted and described embodiments employ a TTP system such as a kerberos-type system for generating and delivering short-lived certificates, other systems could also be used for generating and delivering short-lived certificates. It is possible to provide a system in which different facilities are used for generating and for delivering the certificates. It is possible to provide a system in which delivery of a short-lived certificate is not necessarily accompanied by delivery of a private key or a kerberos ticket.

It is, in general, possible to use some features of the invention without using others. For example, it is possible to provide a system which generates short-lived certificates without using a simulated Smartcard system or vice versa.

Although it is anticipated that the short-lived certificates will be used in connection authentication, it is possible to use short-lived certificates in connection with other security measures, authorization, encryption or other privacy measures and the like. Although it is anticipated that the short-lived certificates will be used primarily in connection with session-oriented applications (such as Internet sites, browsers or servers controlled using a public key system), it is at least theoretically possible to use short-lived certificates in connection with other uses such as store and forward (e.g., secure electronic mail) uses. Although an example has been provided describing use of Smartcards or simulated Smartcards in connection with intranet or Internet browser access, Smartcards or simulated Smartcards can be used in connection with other items, such as electronic mail ("e-mail"). Although use of a KDC or other system for generating short-lived certificates has been described, it is possible to configure they system to issue moderate-life or (standard) long-lived certificates. Although certificate and/or private key delivery is described as occurring as part of a kerberos AS-REP message, it is possible to provide for delivery separately from the AS-REP message. If desired, the system can be configured to deliver only private key and certificates to the client (i.e. without delivering ticket granting tickets or other tickets), or the system may be configured to allow the user to specify whether delivery of both public key credentials and kerberos tickets, and/or both certificate and private key is needed or desired.

Although the invention has been described by way of a preferred embodiment and certain variations and modifications, other variations and modifications can also be used, the invention being defined by the following claims.

What is claimed is:

1. A computer-implemented method for issuing public key certificates for a user in a network which includes at least a first client computer coupled, by said network to at least a first key distribution computer configured to output tickets according to a ticket protocol, the method comprising:

storing, in a memory accessible to said key distribution computer, at least a public key of said user;

receiving in said client computer at least a first password of said user;

verifying validity of said password in said client computer;

transmitting from said client computer, over said network, to said key distribution computer, at least a first message which includes an indication of the identity of said user;

transmitting at a first time, in response to said first message, from said key distribution computer, over said network, to said client computer, both a ticket according to said ticket protocol and a short-lived public key certificate containing said public key of said user.

2. A computer-implemented method as claimed in claim 1 wherein said ticket protocol is a kerberos protocol.

3. A computer-implemented method as claimed in claim 1 further comprising transmitting, in response to said first message, from said key distribution computer, over said network, to said client computer, a private key of said user corresponding to said public key of said user.

4. A computer-implemented method as claimed in claim 1 wherein said short-lived public key certificate has an expiration time less than about one week after said first time.

5. A computer-implemented method as claimed in claim 1 wherein said short-lived public key certificate has an expiration time less than about 12 hours after said first time.

6. A computer-implemented method as claimed in claim 1 further comprising using said short-lived public key certificate to provide authentication of said user.

7. A computer-implemented method as claimed in claim 1 further comprising using said short-lived public key certificate for authorizing said user to use a resource which is controlled by a public key system.

8. A computer-implemented method as claimed in claim 1 wherein said public key certificate is an X.509 certificate.

9. Apparatus for issuing public key certificates for a user in a network, the network including at least a first client computer coupled, by said network to at least a first key distribution computer configured to output tickets according to a ticket protocol, the apparatus comprising:

a memory, accessible to said key distribution computer, for storing at least a public key of said user;

said client computer and said key distribution computer being programmed to

receive, in said client computer, at least a first password of said user;

verify validity of said password in said client computer;

transmit from said client computer, over said network, to said key distribution computer, at least a first message which includes an indication of the identity of said user;

transmit, at a first time, in response to said first message, from said key distribution computer, over said network, to said client computer, both a ticket according to said ticket protocol and a short-lived public key certificate containing said public key of said user.

10. An apparatus, as claimed in claim 9 wherein said ticket protocol is a kerberos protocol.

11. Apparatus as claimed in claim 9, said key distribution computer configured to further transmit, in response to said first message, from said key distribution computer, over said network, to said client computer, a private key of said user corresponding to said public key of said user.

12. Apparatus as claimed in claim 9 wherein said short-lived public key certificate has an expiration time less than about one week after said first time.

13. Apparatus as claimed in claim 9 wherein said short-lived public key certificate has an expiration time less than about 12 hours after said first time.

14. Apparatus as claimed in claim 9 further comprising using said short-lived public key certificate to provide authentication of said user.

15. Apparatus as claimed in claim 9 further comprising using said short-lived public key certificate for authorizing said user to use a resource which is controlled by a public key system.

16. Apparatus, as claimed in claim 9 wherein said public key certificate is an X.509 certificate.

17. Apparatus for issuing public key certificates for a user in a network which includes at least a first client computer coupled, by said network to at least a first key distribution computer configured to output tickets according to a ticket protocol, the method comprising:

memory means, accessible to said key distribution computer, for storing at least a public key of said user;

means, coupled to said client computer, for receiving at least a first password of said user;

means, in said client computer, for verifying validity of said password;

means, coupled to said client computer, for transmitting from said client computer, over said network, to said key distribution computer, at least a first message which includes an indication of the identity of said user;

means, in said key distribution computer, for generating and transmitting at a first time, in response to said first message, from said key distribution computer, over said network, to said client computer, both a ticket according to said ticket protocol and a short-lived public key certificate containing said public key of said user.

18. Apparatus as claimed in claim 17 further comprising means for transmitting, in response to said first message, from said key distribution computer, over said network, to said client computer, a private key of said user corresponding to said public key of said user.

19. Apparatus, as claimed in claim 17, wherein said short-lived public key certificate has an expiration time less than about one week after said first time.

20. Apparatus, as claimed in claim 17 wherein said short-lived public key certificate has an expiration time less than about 12 hours after said first time.

21. Apparatus as claimed in claim 17 further comprising using said short-lived public key certificate to provide authentication of said user.

22. Apparatus as claimed in claim 17 further comprising using said short-lived public key certificate for authorizing said user to use a resource which is controlled by a public key system.

23. Apparatus as claimed in claim 17 wherein said public key certificate is an X.509 certificate.

24. A computer-implemented method for issuing public key certificates for a user comprising:

storing, in a memory coupled to said computer, a plurality of public keys, including a public key associated with said user;

receiving, in said computer, at a plurality of arbitrary times, messages which include an identification of said user;

outputting, in response to each of at least a first plurality of said messages, a public key certificate for said user including an indication of said public key associated with said user and an indication of an expiration time for said certificate, wherein a sequence of public key certificates are output which have identical indication of public key but different and sequential expiration times.

25. A computer-implemented method as claimed in claim 24 wherein a private key of said user corresponding to said public key of said user is output substantially whenever said public key certificate is output.

26. A computer-implemented method as claimed in claim 24 wherein, each public key certificate in said sequence has a validity period extending from substantially when said certificate is output until, the expiration time of said public key certificate, and wherein each public key certificate in said sequence has a validity period of less than about one week so that said sequence of public key certificates is a sequence of short-lived certificates.

27. A computer- implemented method as claimed in claim 24 wherein each of said public key certificates in said sequence has a validity period of less than about one day.

28. A computer-implemented method as claimed in claim 24 wherein each of said public key certificates in said sequence has a validity period of less than about 12 hours.

29. Apparatus for issuing public key certificates for a user comprising:

a memory coupled to a computer, for storing a plurality of public keys, including a public key associated with said user;

said computer being programmed to have the capability of receiving, at a plurality of arbitrary times, messages which include an identification of said user;

said computer being programmed to output, in response to each of at least a first plurality of said messages, a public key certificate for said user including an indication of said public key associated with said user and an indication of an expiration time for said certificate, wherein a sequence of public key certificates are output which have identical indication of public key but different and sequential expiration times.

30. Apparatus as claimed in claim 29 wherein said computer is programmed such that a private key of said user corresponding to said public key of said user is output substantially whenever said public key certificate is output.

31. Apparatus as claimed in claim 29 wherein each public key certificate in said sequence has a validity period extending from substantially when said certificate is output until, the expiration time of said public key certificate, and wherein each public key certificate in said sequence has a validity period of less than about one week so that said sequence of public key certificates is a sequence of short-lived certificates.

32. Apparatus as claimed in claim 29 wherein each of said public key certificates in said sequence has a validity period of less than about one day.

33. Apparatus as claimed in claim 29 wherein each of said public key certificates in said sequence has a validity period of less than about 12 hours.

34. Apparatus for issuing public key certificates for a user comprising:

memory means, coupled to a computer, for storing a plurality of public keys, including a public key associated with said user;

said computer being programmed to receive, at a plurality of arbitrary times, messages which include an identification of said user;

said computer being programmed to output, in response to each of at least a first plurality of said messages, a public key certificate for said user including an indication of said public key associated with said user and an indication of an expiration time for said certificate, wherein a sequence of public key certificates are output which have identical indication of public key but different and sequential expiration times.

35. Apparatus as claimed in claim 34 further comprising means for outputting a private key of said user corresponding to said public key of said user substantially whenever said public key certificate is output.

36. Apparatus as claimed in claim 34 wherein, each public key certificate in said sequence has a validity period extending from substantially when said certificate is output until, the expiration time of said public key certificate, and wherein each public key certificate in said sequence has a validity period of less than about one week so that said sequence of public key certificates is a sequence of short-lived certificates.

37. A computer- implemented method as claimed in claim 36 wherein each of said public key certificates in said sequence has a validity period of less than about one day.

38. A computer-implemented method as claimed in claim 36 wherein each of said public key certificates in said sequence has a validity period of less than about 12 hours.

39. A computer-implemented method for issuing public key certificates for a user comprising:

receiving, in said computer, a messages which include an identification of said user;

outputting, in response to said step of receiving, a short-lived public key certificate.

40. Apparatus for issuing public key certificates for a user comprising:

a computer programmed to receive messages which include an identification of said user and to output, in response to said messages, short-lived public key certificates.

41. Apparatus for issuing public key certificates for a user comprising:

computer-implemented means for receiving messages which include an identification of said user;

computer-implemented means for outputting short-lived public key certificates in response to receiving said messages.

42. In a computer-implemented authentication system configured to authenticate users in accordance with a first Smartcard protocol, a method for authenticating to a resource comprising:

providing a public/private key pair of a first user; and

using said key pair to simulate the response which a Smartcard generates in accordance with said Smartcard protocol.

43. A method as claimed in claim 42 wherein the public key of said public/private key pair is certified by an unexpired short-lived public key certificate of said user.

44. A computer-implemented public-key certification method comprising:

obtaining a public-key and private-key pair;

generating a series of public-key certificates for said public-key, with a frequency of at least two public-key certificates per year.

45. A method, as claimed in claim 44, wherein said frequency is at least about 12 public-key certificates per year.

46. A method, as claimed in claim 44, wherein said frequency is at least about five public-key certificates per week.

47. A method, as claimed in claim 44 wherein said public-key certificates include an expiration defining a certificate lifetime of less than about six months.

48. A method, as claimed in claim 44, wherein said public-key certificates include an expiration defining a certificate lifetime of less than about one week.

49. A method, as claimed in claim 44, wherein said public-key private-key pair has an expiration defining a public-key private-key lifetime of at least about one year.

50. A method, as claimed in claim 44, wherein said public-key private-key pair has an expiration defining a public-key private-key lifetime of less than about one day.

51. A method, as claimed in claim 50, wherein said public-key certificates include an expiration defining a certificate lifetime of less than about one day.

52. A method, for use in a computer system having at least one client computer and at least one server computer coupled by a communications link, the method comprising:

storing in a memory coupled to said computer system, first information representing at least some data of a type normally stored on a smart card;

using a kerberos-like system for password-based authentication of a user to said server; and

retrieving said first information following said password-based authentication..

53. A method, as claimed in claim 52, further comprising using said first information to simulate use of a hardware Smartcard.

54. A method, as claimed in claim 52, wherein said first information includes at least one of a symmetric key, an asymmetric key pair, and a key certificate.

55. A method, as claimed in claim 44, wherein said public key certificates further include authorization information.

56. A method, as claimed in claim 55, wherein said authorization information includes group affiliation information.

57. A method, as claimed in claim 56, further comprising using said authorization information in a resource authorization system.

58. Apparatus for user authentication comprising:

means for receiving a hardware Smartcard and using said received hardware Smartcard to authenticate a user; and

means for simulating a hardware Smartcard, in the absence of a hardware Smartcard, to authenticate a user.

59. A computer-implemented method for simulating logging in to a physical smartcard, comprising:

prompting, by a client computer, for a password from a user in response to a client application login request;

sending a message to at least a first server computer which includes a request identifying the user, in the absence of sending said password to said server computer;

sending, from said server computer to said client computer, a smartcard image, at least partially encrypted; and

sending a message to said client application to simulate a response from a physical smartcard, using at least some information from said smartcard image.

60. A method, as claimed in claim 59, wherein said smartcard image includes a public key certificate, and further comprising:

determining if said public key certificate is expired;

sending a certification request to a server computer when said public key certificate is expired.

61. A method, as claimed in claim 59, further comprising:

transmitting information from said client computer to said first server computer for updating said smartcard image.

62. Apparatus for simulating logging in to a physical smart-card, comprising:

means for prompting, by a client computer, for a password from a user in response to a client application login request;

means for sending a message to at least a first server computer which includes a request identifying the user, in the absence of sending said password to said server computer;

means for sending, from said server compuer to said client computer, a smartcard image, at least partially encrypted; and

means for sending a message to said client application to simulate a response from a physical smartcard, using at least some information from said smartcard image.

63. Apparatus for simulating logging in to a physical smartcard in a network, the network including at least a first client computer coupled, by said network, to at least a first server computer, comprising:

a memory, accessible to said server computer, for storing information representative of at least a first smartcard image;

said client and server computers being programmed to

prompt, by said client computer, for a password from a user in response to a client application login request;

send a message to at least said first server computer which includes a request identifying the user, in the absence of sending said password to said server computer;

send, from said server compuer to said client computer, a smartcard image, at least partially encrypted; and

send a message to said client application to simulate a response from a physical smartcard, using at least some information from said smartcard image.

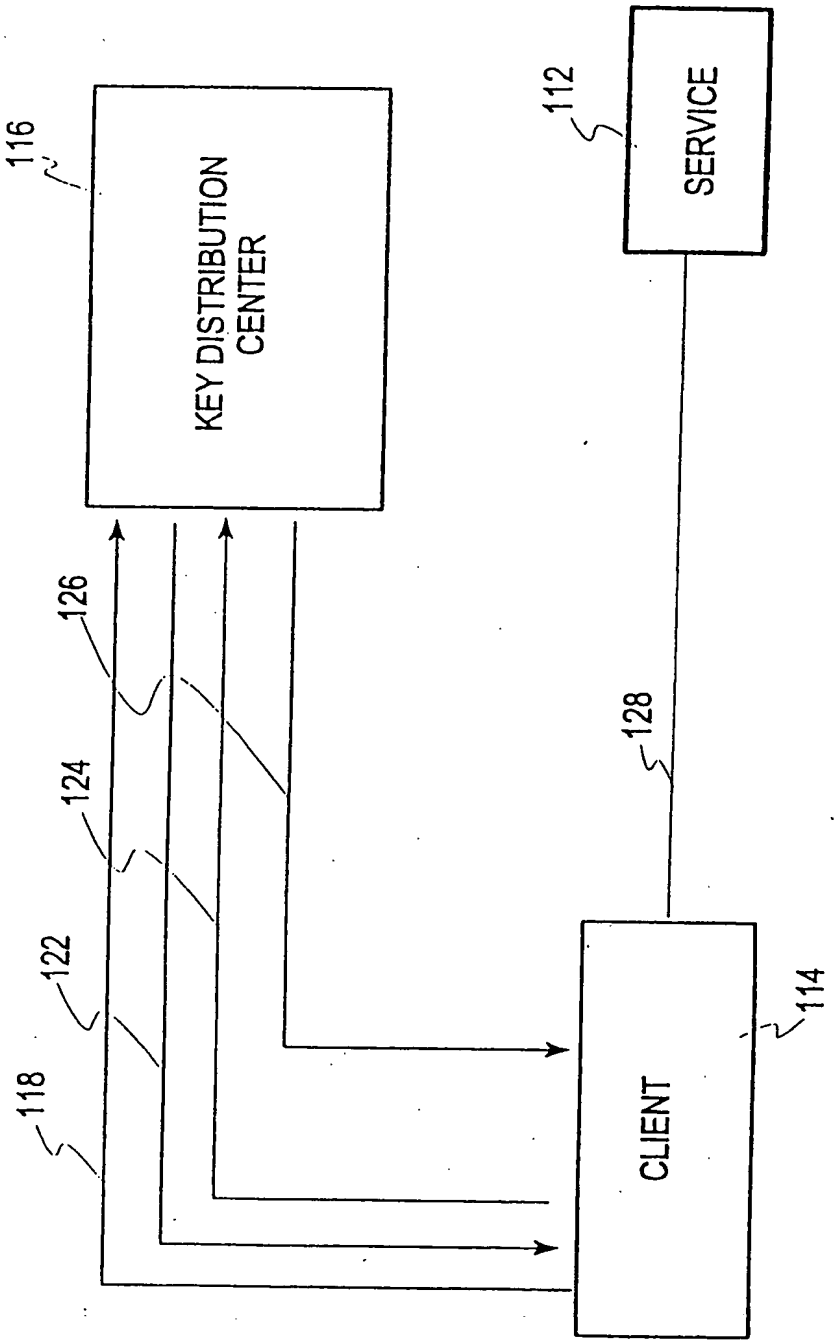


FIG. 1
Prior Art

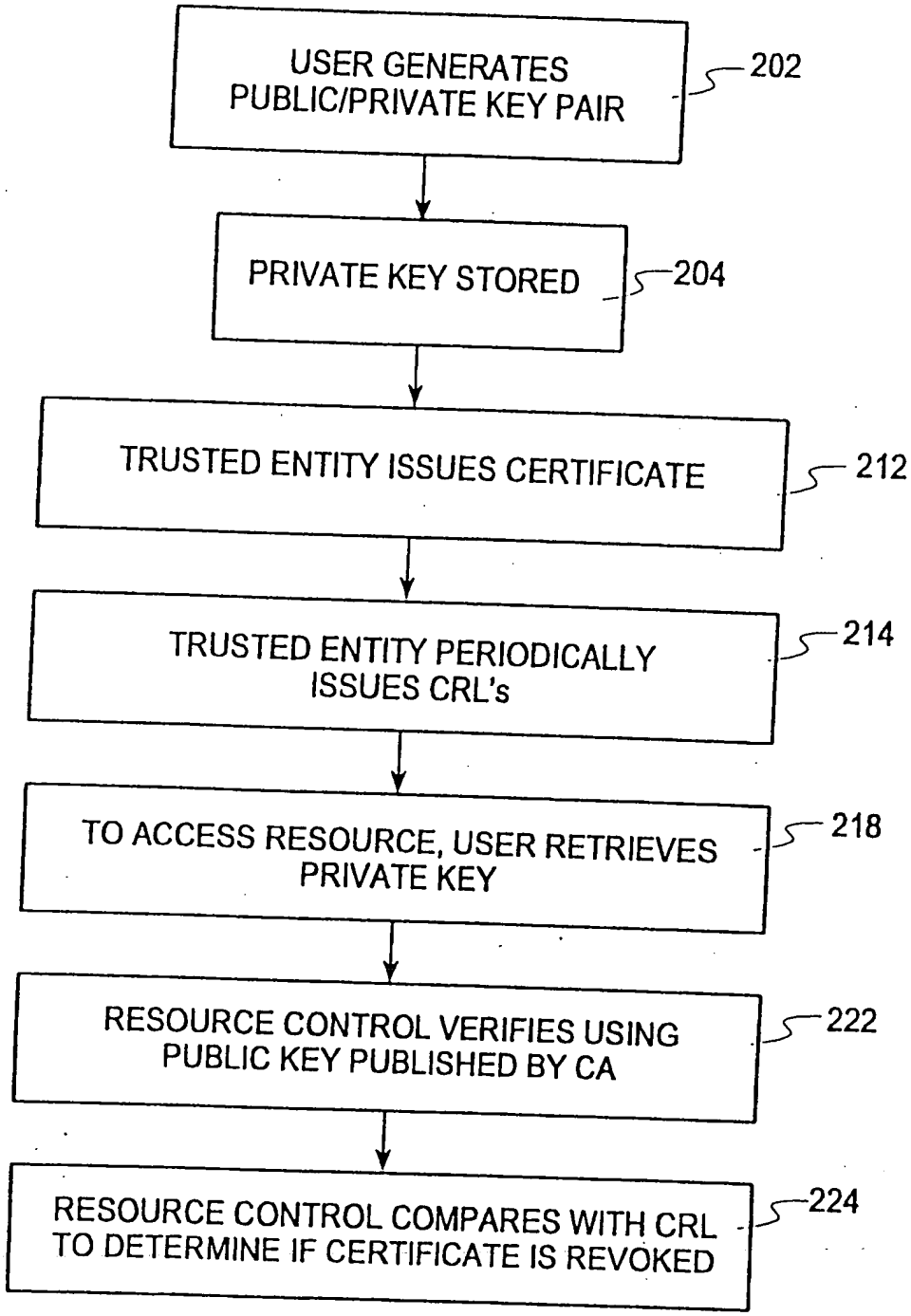


FIG. 2
Prior Art

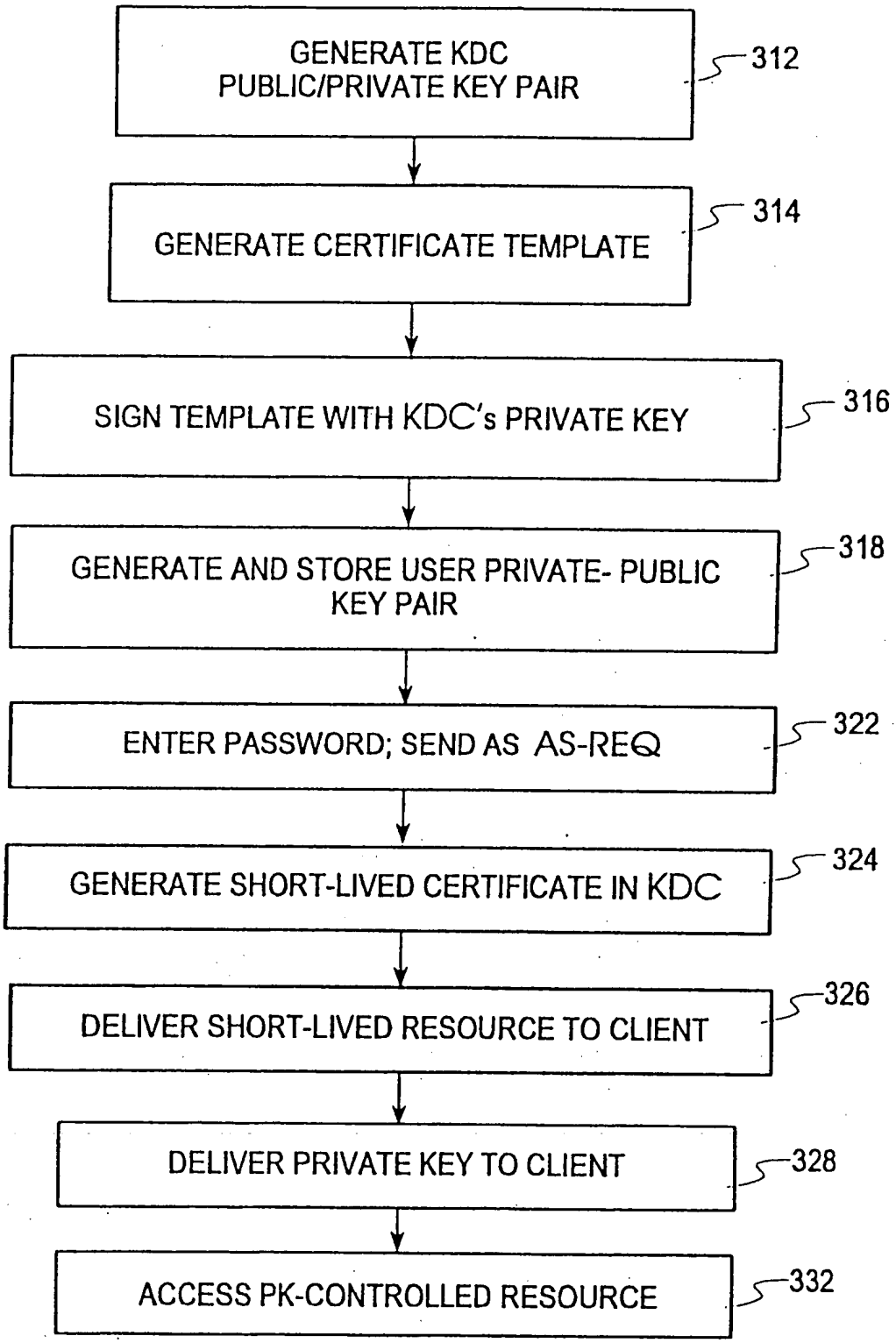

GENERATE KDC PUBLIC/PRIVATE KEY PAIR
312
GENERATE CERTIFICATE TEMPLATE
314
SIGN TEMPLATE WITH KDC's PRIVATE KEY
316
GENERATE AND STORE USER PRIVATE- PUBLIC KEY PAIR
318
ENTER PASSWORD; SEND AS AS-REQ
322
GENERATE SHORT-LIVED CERTIFICATE IN KDC
324
DELIVER SHORT-LIVED RESOURCE TO CLIENT
326
DELIVER PRIVATE KEY TO CLIENT
328
ACCESS PK-CONTROLLED RESOURCE
332

FIG. 3

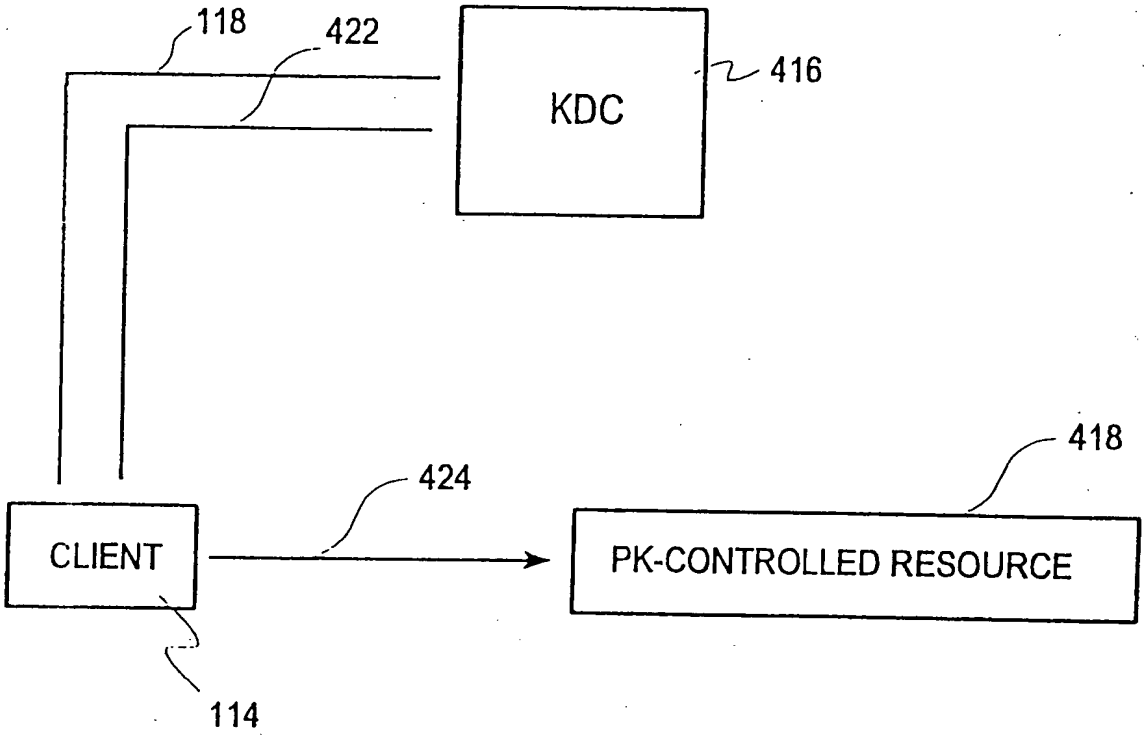


FIG. 4

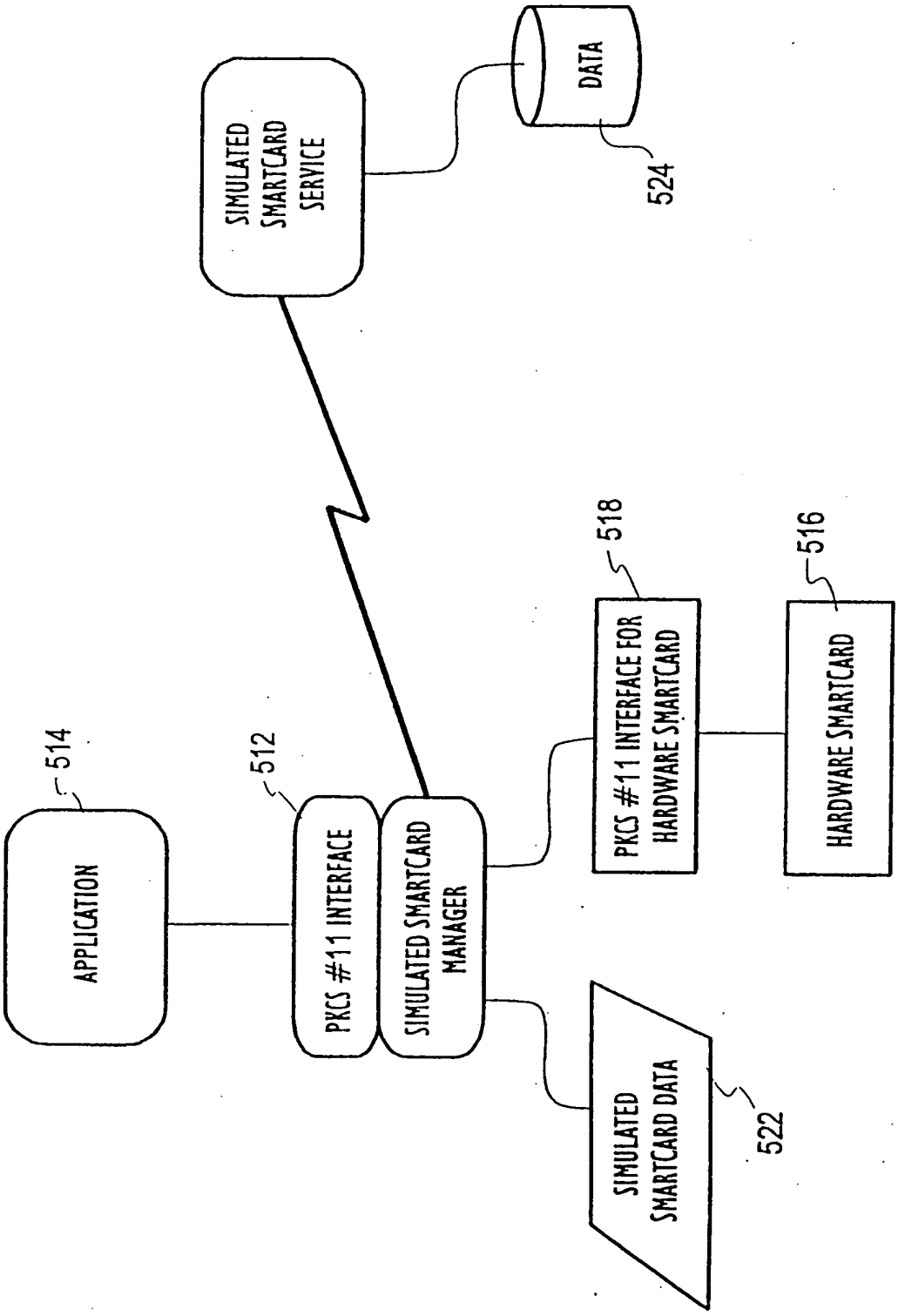

APPLICATION
514
PKCS #11 INTERFACE
512
SIMULATED SMARTCARD MANAGER
SIMULATED SMARTCARD SERVICE
DATA
524
PKCS #11 INTERFACE FOR HARDWARE SMARTCARD
518
HARDWARE SMARTCARD
516
SIMULATED SMARTCARD DATA
522

FIG. 5

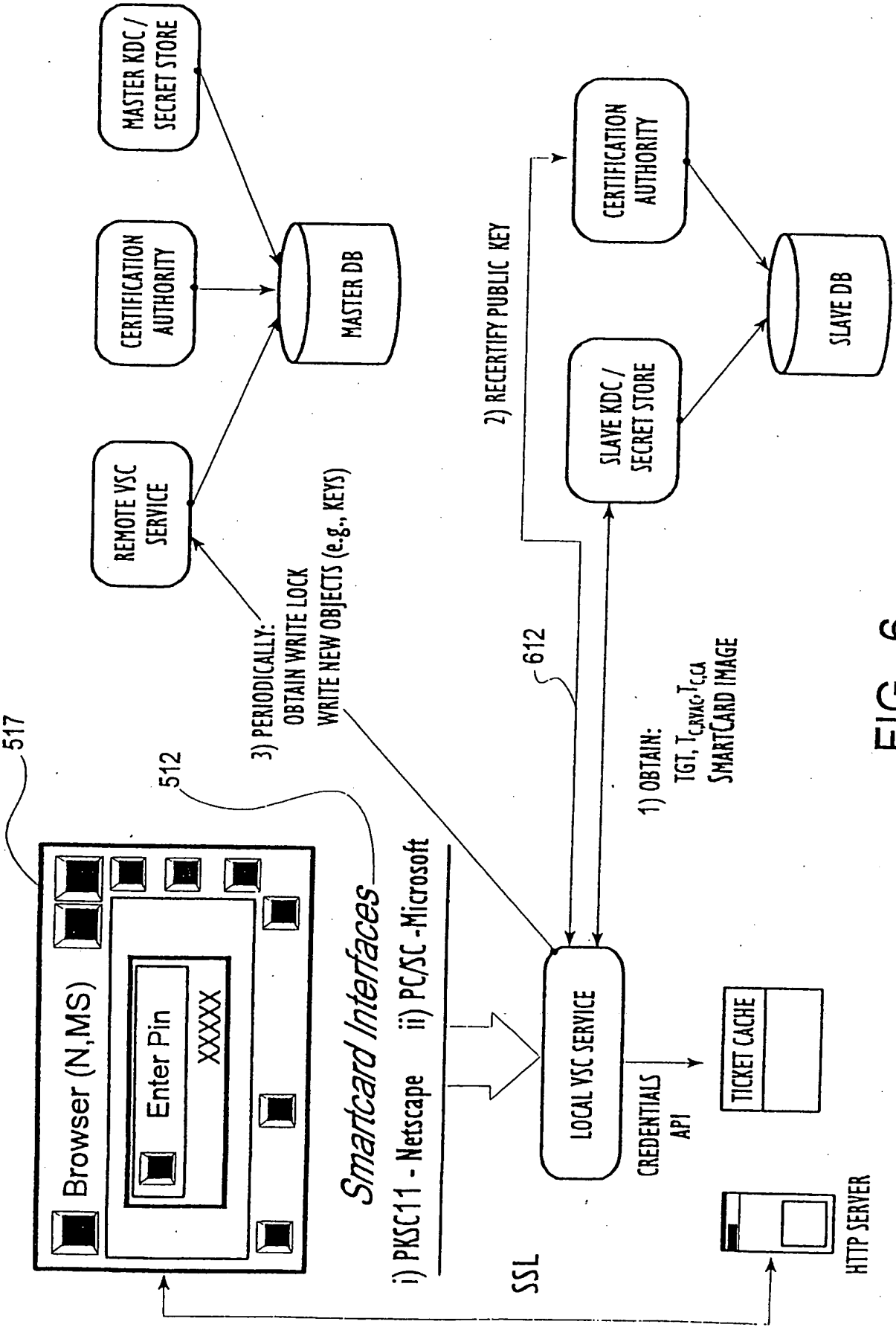

MASTER KDC / SECRET STORE
CERTIFICATION AUTHORITY
MASTER DB
REMOTE VSC SERVICE
3) PERIODICALLY:
OBTAIN WRITE LOCK
WRITE NEW OBJECTS (e.g., KEYS)
2) RECERTIFY PUBLIC KEY
CERTIFICATION AUTHORITY
SLAVE KDC / SECRET STORE
SLAVE DB
612
1) OBTAIN:
TGT, $T_{C,RVKC}$, $T_{C,CA}$
SMARTCARD IMAGE
517
512
Browser (N,MS)
Enter Pin
XXXXX
Smartcard Interfaces
i) PKSC11 - Netscape ii) PC/SC -Microsoft
LOCAL VSC SERVICE
CREDENTIALS API
TICKET CACHE
SSL
HTTP SERVER

FIG. 6

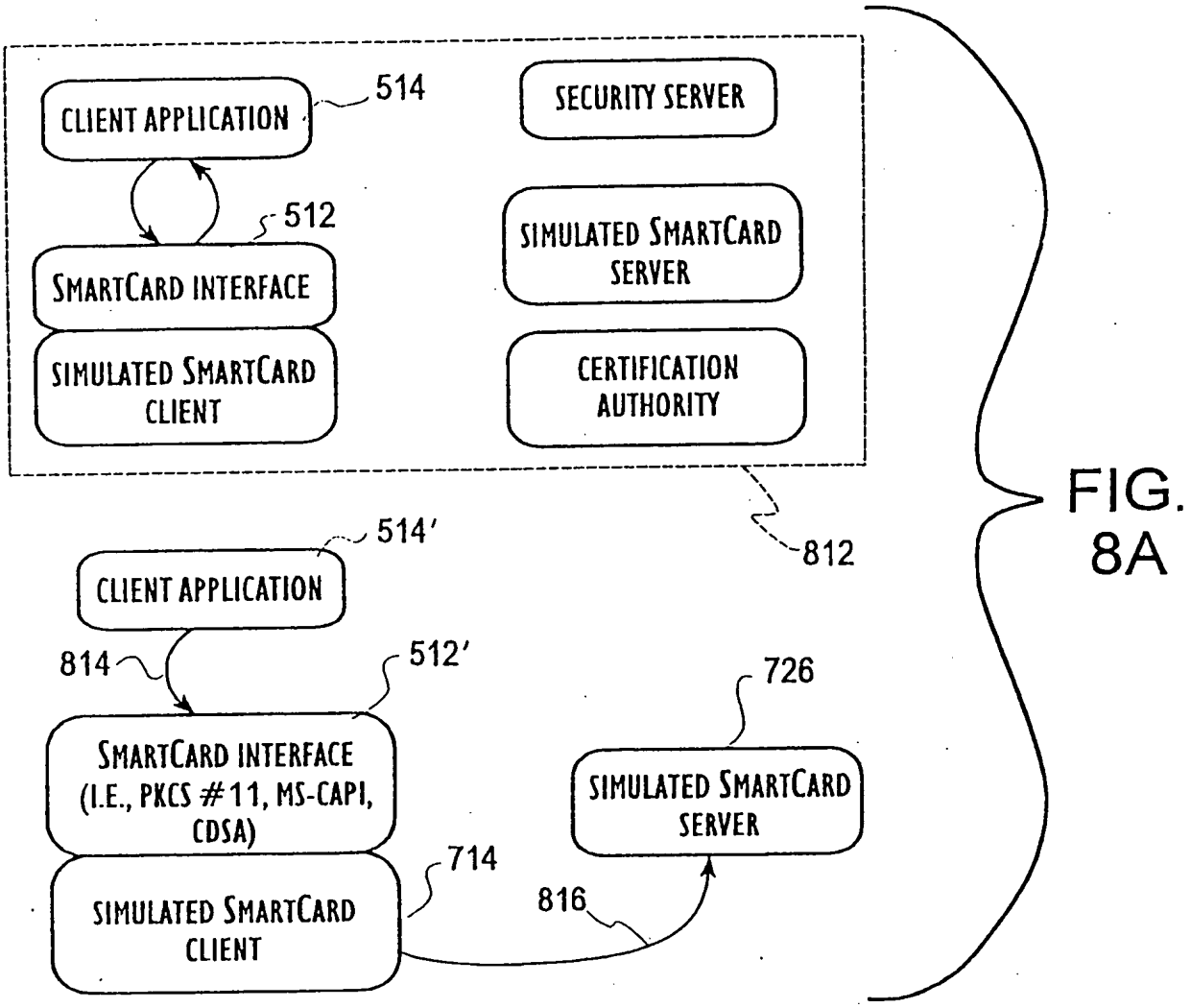

CLIENT APPLICATION
514
SECURITY SERVER
512
SMARTCARD INTERFACE
SIMULATED SMARTCARD SERVER
SIMULATED SMARTCARD CLIENT
CERTIFICATION AUTHORITY
812
514'
CLIENT APPLICATION
814
512'
726
SMARTCARD INTERFACE (I.E., PKCS #11, MS-CAPI, CDSA)
SIMULATED SMARTCARD SERVER
714
SIMULATED SMARTCARD CLIENT
816

FIG. 8A

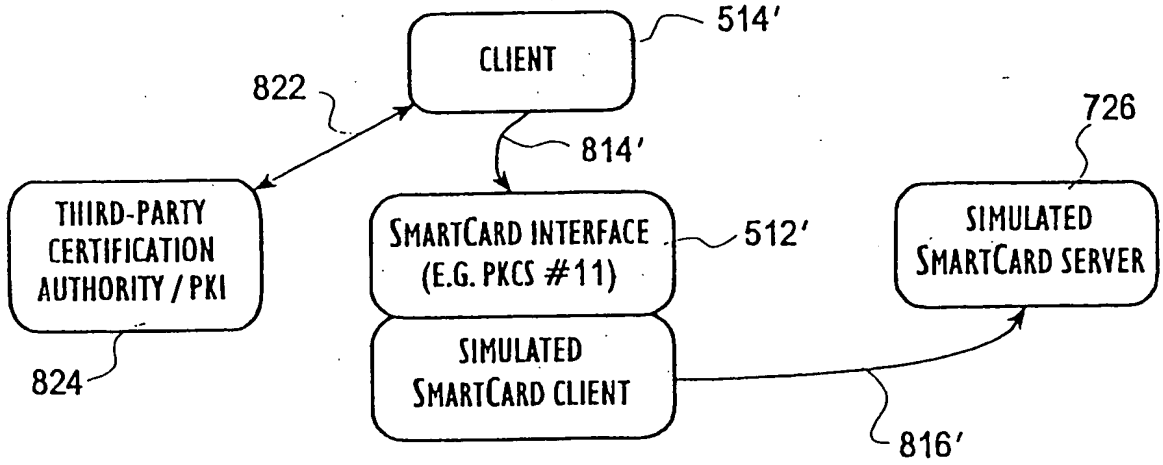

CLIENT
514'
822
814'
726
THIRD-PARTY CERTIFICATION AUTHORITY / PKI
SMARTCARD INTERFACE (E.G. PKCS #11)
512'
SIMULATED SMARTCARD SERVER
SIMULATED SMARTCARD CLIENT
824
816'

FIG. 8B

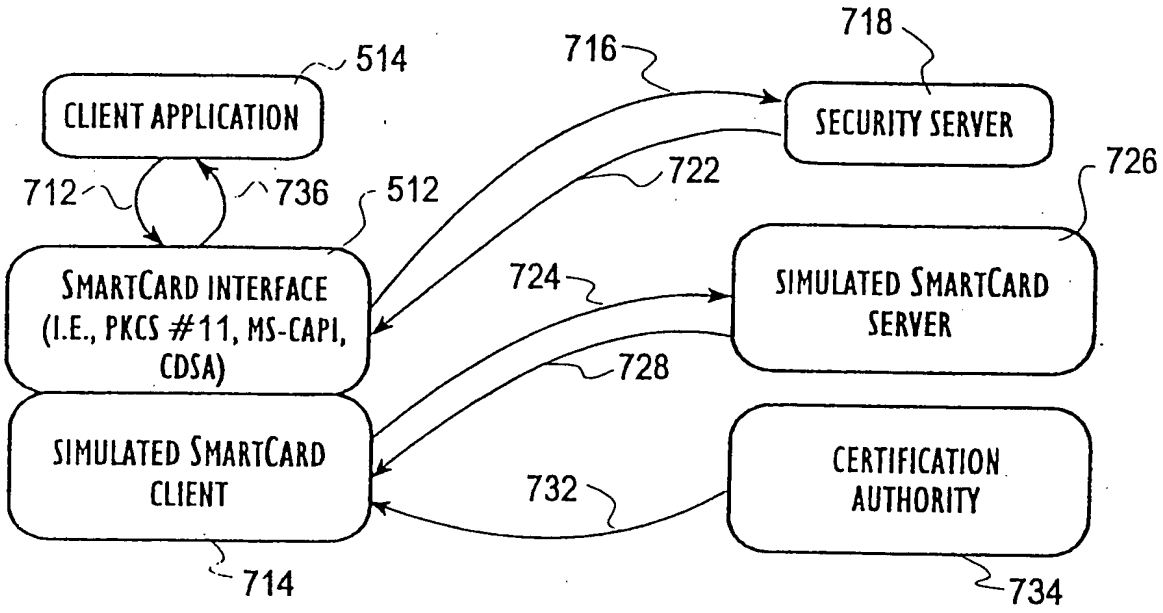

514
CLIENT APPLICATION
716
718
SECURITY SERVER
712
736
512
722
726
SMARTCARD INTERFACE (I.E., PKCS #11, MS-CAPI, CDSA)
724
SIMULATED SMARTCARD SERVER
728
SIMULATED SMARTCARD CLIENT
732
CERTIFICATION AUTHORITY
714
734

FIG. 7

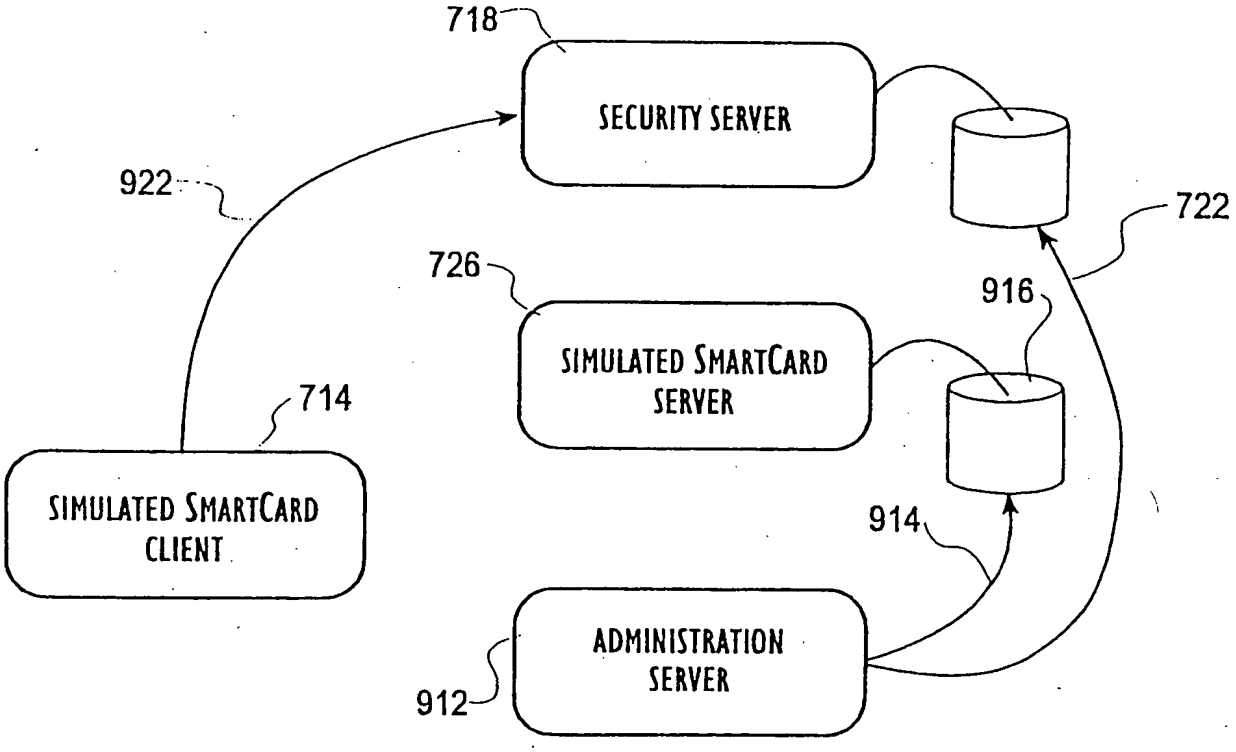

718
SECURITY SERVER
922
722
726
916
SIMULATED SMARTCARD SERVER
714
SIMULATED SMARTCARD CLIENT
914
ADMINISTRATION SERVER
912

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/00344

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/30; G06F 13/362
US CL :380/25, 30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/25, 30, 21, 49

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS: authenticat? and certificat?; simulat?(2w)(smart card or intelligent token)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US 5,737,419 A (GANESAN) 07 APRIL 1998, see col. 5, lines 20-24.	1-51
A	US 5,200,999 A (MATYAS et al.) 06 APRIL 1993, see col. 90, lines 30-33.	1-51.
A	US 5,687,235 A (PERLMAN et al.) 11 NOVEMBER 1997, see col. 2, lines 24-45.	1-51
Y	US 5,347,580 A (MOLVA et al.) 13 SEPTEMBER 1994, see col. 6, lines 21-48.	52-63
Y	US 5,521,966 A (FRIEDES et al.) 28 MAY 1996, see col. 5, lines 43-55.	52-63
A	US 5,655,077 A (JONES et al.) 05 AUGUST 1997, see col. 2, lines 47-58.	52-63

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
01 APRIL 1999

Date of mailing of the international search report
20 MAY 1999

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
GILBERTO BARRÓN JR.
Telephone No. (703) 305-1830

Form PCT/ISA/210 (second sheet)(July 1992)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/00344

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US 5,774,552 A (GRIMMER) 30 JUNE 1998, see col.9, lines 10-15.	1-51

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/00344

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/00344

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING

This ISA found multiple inventions as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single inventive concept under PCT Rule 13.1. In order for all inventions to be searched, the appropriate additional search fees must be paid.

Group I, claim(s) 1-51, drawn to method and apparatus for issuing public key certificates.
Group II, claim(s) 52-63, drawn to method and apparatus for simulating logging in to a smartcard.
The inventions listed as Groups I and II do not relate to a single inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: Group I provides for the special technical feature of a short lived certificate not required in Group II. Group II provides for the special technical feature of simulating logginh in to a physical smartcard bot required in Group I.